

**IN THE UNITED STATES BANKRUPTCY COURT  
FOR THE DISTRICT OF DELAWARE**

In re

Chapter 11

Zen JV, LLC, *et al.*,<sup>1</sup>

Case No. 25-11195 (JKS)

Debtors.

(Jointly Administered)

**CONSUMER PRIVACY OMBUDSMAN REPORT**

Alan Chapell, Esq., CIPP  
Chapell & Associates, LLC  
92 Warren Street, #11, New York, NY 10007  
Telephone: (917) 318-8440  
achapell@chapellassociates.com  
Date: July 16, 2025

---

<sup>1</sup> The Debtors in these cases, along with the last four digits of each debtor's federal tax identification number (to the extent applicable), are: Zen JV, LLC (0225); Monster Worldwide LLC (6555); FastWeb, LLC; Monster Government Solutions, LLC (5762); Camaro Acquisition, LLC; CareerBuilder, LLC (6495); CareerBuilder Government Solutions, LLC (6426); Luceo Solutions, LLC (4426); CareerBuilder France Holding, LLC (9339); and Military Advantage, LLC (9508). The Debtors' address is 200 N LaSalle Street #900, Chicago, IL 60601.

## TABLE OF CONTENTS

Introduction .....	1
Summary of Findings and Recommendation .....	3
Included Data Categories .....	3
Excluded Data Categories .....	5
Debtors’ PII Collection and Processing .....	7
Additional Background Information .....	8
Sensitive Data .....	9
Recommendations .....	10
Applicable Consumer Privacy and Data Protection Laws .....	11
U.S. Federal Laws .....	12
Applicable U.S. State Laws.....	19
Non-U.S. Laws .....	23
The Debtors’ Consumer Privacy Policies and Practices .....	24
Factors to Be Considered.....	25
Recommendations .....	26

**TABLE OF EXHIBITS**

EXHIBIT A	CareerBuilder Privacy Policy July 2025
EXHIBIT B	CareerBuilder Privacy Policy September 2023
EXHIBIT C	CareerBuilder Privacy Policy March 2018
EXHIBIT D	Fastweb Privacy Policy July 2025
EXHIBIT E	Fastweb Privacy Policy April 2020
EXHIBIT F	Fastweb Privacy Policy January 2017
EXHIBIT G	Finaid Privacy Policy July 2025
EXHIBIT H	Finaid Privacy Policy January 2019
EXHIBIT I	Military Privacy Policy July 2025
EXHIBIT J	Military Privacy Policy February 2022
EXHIBIT K	Monster Privacy Policy July 2025
EXHIBIT L	Monster Privacy Policy April 2021
EXHIBIT M	Monster Privacy Policy January 2013
EXHIBIT N	FTC v. Toysmart.com Proposed Stipulation and Settlement

Alan Chapell, the Consumer Privacy Ombudsman, duly appointed pursuant to section 332 of the Bankruptcy Code,<sup>2</sup> respectfully submits this Report to the Court and states:

### **Introduction**

1. On July 8, 2025, the United States Trustee filed the *Notice of Appointment of Consumer Privacy Ombudsman*, along with the Ombudsman's acceptance of appointment and verified statement of disinterestedness (Docket No. 106).

2. The Ombudsman has prepared this Report in accordance with Section 363(b)(1)(B) of the Bankruptcy Code to assist the Court in its consideration of the facts, circumstances, and conditions of the sale by Debtors of its customers' Personally Identifiable Information ("PII").

3. The purpose of this Report is to provide the Court with the information specified in section 332(b) of the Bankruptcy Code and to assist the Court in understanding the "applicable nonbankruptcy law" referenced in section 363(b)(1)(B)(ii) of the Bankruptcy Code.<sup>3</sup>

4. In preparing this Report, the Ombudsman has, among other things:

- a. Reviewed the draft *Asset Purchase Agreements* of Alsoft Corporation, Inc., Valnet Us Inc., and JobGet Inc.;
- b. Reviewed the CareerBuilder privacy statement currently posted online at the Debtors' website, [www.CareerBuilder.com](http://www.CareerBuilder.com), as well as two previously posted privacy statements via the Internet Archive at [www.archive.org](http://www.archive.org), attached as **Exhibit A, Exhibit B, and Exhibit C**, respectively;

---

<sup>2</sup> 11 U.S.C. §332 (2006).

<sup>3</sup> Pursuant to the Bankruptcy Code, the Consumer Privacy Ombudsman may provide this Court with information relating to (1) the Debtors' privacy policy; (2) the potential losses or gains of privacy to consumers if a sale or lease is approved by the Court; (3) the potential costs or benefits to consumers if a sale or lease is approved by the Court; and (4) the potential alternatives that would mitigate potential privacy losses or potential costs to consumers. 11 USC § 332 (2006).

- c. Reviewed the Fastweb privacy statement currently posted online at the Debtors' website, [www.Fastweb.com](http://www.Fastweb.com), as well as two previously posted privacy statements via the Internet Archive at [www.archive.org](http://www.archive.org), attached as **Exhibit D, Exhibit E, and Exhibit F**, respectively;
- d. Reviewed the Finaid privacy statement currently posted online at the Debtors' website, [www.Finaid.org](http://www.Finaid.org), as well as a previously posted privacy statement via the Internet Archive at [www.archive.org](http://www.archive.org), attached as **Exhibit G, and Exhibit H**, respectively;
- e. Reviewed the Military privacy statement currently posted online at the Debtors' website, [www.Military.com](http://www.Military.com), as well as two previously posted privacy statements via the Internet Archive at [www.archive.org](http://www.archive.org), attached as **Exhibit I, and Exhibit J**, respectively;
- f. Reviewed the privacy statement governing both Monster and Monster Government Solutions currently posted online at the Debtors' websites, [www.Monster.com](http://www.Monster.com) and [www.MonsterGovernmentSolutions.com](http://www.MonsterGovernmentSolutions.com), as well as two previously posted privacy statements via the Internet Archive at [www.archive.org](http://www.archive.org), attached as **Exhibit K, Exhibit L, and Exhibit M**, respectively;
- g. Examined the data collection functions of Debtors' social media programs, including but not limited to information collected via Debtors' Facebook, Instagram, X, Pinterest, YouTube, and TikTok pages and accounts;
- h. Discussed, via email and telephone conversations with Debtors' Counsel, Debtors' PII-collection activities, practices, and the structure of its databases;
- i. Discussed, via email and telephone conversations with Debtors' counsel, the nature

of the data subject to transfer as part of this proceeding; and

- j. Researched applicable United States federal and state privacy laws.

### **Summary of Findings and Recommendation**

5. It is the Consumer Privacy Ombudsman's understanding that Zen JV, LLC, *et al* (hereafter "Debtors" or "Zen") seeks to sell certain customer information to one or more entities, which are yet to be determined<sup>4</sup> (the "Purchaser(s)"), and such customer information includes:

- a. All customer and prospective customer information obtained via Debtors' websites, mobile applications and other digital media properties (collectively "Digital Properties") including from the following URLs: <https://www.monster.com/>; <https://www.monstergovernmentsolutions.com/>; <https://www.fastweb.com/>, <https://www.military.com/>; <https://findaid.org/>; <https://www.careerbuilder.com/>.
- b. All of Debtors' social media account information (e.g., list of X and Instagram followers, Facebook likes) associated with each of those Digital Properties on the following social media platforms: <https://x.com/>; <https://www.instagram.com/>; <https://www.facebook.com/>; <https://www.pinterest.com/>; <https://www.tiktok.com/>, and <https://www.linkedin.com/> (collectively, Debtors' Social Media Accounts).

### **Included Data Categories**

6. It is the Consumer Privacy Ombudsman's understanding that Debtors seek to transfer information obtained via Debtors' Social Media Accounts and via Debtors' Digital Properties;

---

<sup>4</sup> It is the Privacy Ombudsman's understanding that as of July 15, 2025, there are three stalking horses bidders (Alsoft Corporation, Inc., Valnet Us Inc., and JobGet Inc.) that could purchase Debtors' PII pursuant to this proceeding. Other companies may make bids in as part of the process.

7. Debtors' Digital Properties collected the following categories of information of job applicants, prospective job applicants, employers and recruiters:

- a. Browsing information and similar pseudonymous personal data, including: IP addresses, browser and device type collected from the device of visitors to Debtor's Digital Properties;<sup>5</sup>
- b. Broad geolocation data (city or postal code) derived from the IP address of a visitor's device;
- c. Commercial information, including: business address, business email, and business phone number;
- d. Contact information, including: Names, contact details, home addresses, personal emails, phone numbers, and previous residence addresses;
- e. Personal identification information, including: First name, last name, account name, age, aliases, date of birth, gender, marital status, nationality, race or ethnic origin, unique personal identifiers;
- f. Disposition data, including: decisions made by jobseekers and employers/recruiters relative to job applications, such as whether to grant an interview, make a job offer or to accept or reject an interview and/or offer;

---

<sup>5</sup> The Bankruptcy Code as amended under Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 defines "PII" narrowly so as to include identifiable personal data (e.g., email, postal address, phone number, bank account number), the FTC, U.S. State privacy laws and the (more generally) courts have increasingly defined "PII" / "personal data" much more broadly so as to include pseudonymous personal data such as "IP address" and pseudonymous advertising identifiers within the scope of the definition. The Privacy Ombudsman follows the lead of each of the aforementioned authorities in also adopting a broad definition of personal data in the CPO Report definition of PII.

- g. Education and skills, including: job applicant's academic performance, (e.g., grade point average), education history, degrees, languages spoken, job/employment training history;
- h. Employment Information, including: business unit or division name, company name, employment type (contract, term, temporary), hire and end date, job title or role, office location, previous work history, salary or wage, interview history and status, and compensation data (e.g., salary / bonus);
- i. Professional affiliations information, including: Professional certifications, trade group associations or memberships;
- j. Profiles, inferences and generated data, including: Inferred contact information, demographic information like age, work experience, salary, race or ethnic origin;
- k. Social media data from jobseekers, including: Profile username, first name, last name, contact information, profile picture, post history;
- l. User account data, including: Account username, account password;
- m. Information from Debtor's Social Media Accounts (e.g., list of Twitter followers and Facebook likes).

### **Excluded Data Categories**

8. PII for which Debtor operates as a data processor - It is the Consumer Privacy Ombudsman's understanding that, with the exception of PII collected via "contact us" forms on the website located at <https://www.monstergovernmentalsolutions.com/>, the data managed by Debtors via its Monster Governmental Solutions team ("MGS") is outside the scope of this evaluation. Debtor (via Debtor's counsel) has represented to the Consumer Privacy



Ombudsman that MGS operates as a data “processor” (under the Colorado Privacy Act and similar privacy laws) and a “service provider” (under the California Consumer Privacy Act and similar privacy laws) - meaning that MGS is bound by written contract to process that subset of PII solely as instructed by Debtors’ customers (which are generally businesses and governmental entities).<sup>6</sup> It is the Consumer Privacy Ombudsman’s further understanding that there are additional PII for which Debtors operate as a data processor and/or service provider – in addition to the PII processed via MGS (e.g., where Debtors offered a white-label version of its services). Provided that the Debtors’ business and government customers (and not Debtors) each continue to make any and all processing decisions with respect to such subset of PII, there is no potential change in privacy practices for the Ombudsman to review. Accordingly, the Privacy Ombudsman is not offering an opinion with respect to that subset of PII.

9. B2B Data - It is the Consumer Privacy Ombudsman’s understanding there is an additional subset of PII collected by Debtors’ pursuant to Debtors’ role working with its business and/or government customers in their respective role as employers. This business-to-business data set processed by Debtor includes the employers’ company name, contact information for the employers’ personnel, and employers’ payment card and bank account information (e.g., to process billing and facilitate payment between Debtors’ and such customers). With respect to this data set (the “B2B Data”), Debtors’ counsel correctly noted to the Ombudsman that the definition of “PII” that is applicable here under the Bankruptcy Code is limited to data provided “in connection with obtaining a product or a service from the debtor primarily for personal,

---

<sup>6</sup> For a more thorough description of the terms “data processor” and “service provider”, please see the section of the CPO Report entitled “Applicable Consumer Privacy and Data Protection Laws.

family, or household purposes”.<sup>7</sup> Accordingly, any B2B Data that Debtors’ process would be outside of the scope of the Ombudsman’s review. The Ombudsman’s view is that adopting a strict interpretation of the definition of PII and the role of the Ombudsman may not be aligned with privacy interests. While the initial impetus for the creation of the role of the Privacy Ombudsman within the Bankruptcy Code was to protect *consumers* from privacy risks, those same or at least similar risks could present themselves in a business-to-business context – particularly if some of the PII within this subset pertain to small and medium sized businesses. Moreover, Courts have recognized that adopting a more flexible approach when it comes to interpreting the Consumer Privacy Ombudsman’s role may be appropriate.<sup>8</sup>

10. The above concern notwithstanding, the Privacy Ombudsman envisions fewer potential privacy issues moving forward with the sale of the B2B Data subset of Debtors’ PII if the Purchaser(s) are each a Qualified Buyer.

### **Debtors’ PII Collection and Processing**

11. Debtors’ Digital Properties and Social Media Accounts collected “personally identifiable information” (“PII”) as defined by Section 101(41A) of the Bankruptcy Code.<sup>9</sup>

---

<sup>7</sup> 11 U.S.C. §101(41A) (2006).

<sup>8</sup> See *In re: 23ANDME HOLDING CO., et al.* No. 25-40976-357 (Bankr. E.D. Missouri). In this bankruptcy proceeding, the debtors’ privacy policy did not place restrictions on the sale of PII pursuant to a bankruptcy. As such, the appointment of a Consumer Privacy Ombudsman was not required under the Bankruptcy statute. Nonetheless, the parties (including the debtor) ultimately agreed that the appointment of a Consumer Privacy Ombudsman was appropriate.

<sup>9</sup> “[P]ersonally identifiable information’ means—

(A) if provided by an individual to the debtor in connection with obtaining a product or a service from the debtor primarily for personal, family, or household purposes—

“(i) the first name (or initial) and last name of such individual, whether given at birth or time of adoption, or resulting from a lawful change of name;

“(ii) the geographical address of a physical place of residence of such individual ...”

11 U.S.C. §101(41A) (2006).

12. While Debtors' did collect the PII of non-US data subjects, such data collected from non-US data subjects will not be subject to transfer pursuant to this proceeding. Should that change, the Ombudsman shall file a supplemental Report.

13. Debtors collected, maintained and used the PII collected pursuant to a privacy policy that limits or restricts the transfer of such assets.

### **Additional Background Information**

14. In general, customer records which contain PII were collected at different times and under different privacy statements – as Debtors updated its privacy policies frequently over time.

15. Overall, with the exception of PII collected via CareerBuilder (discussed below), most of the PII that is subject to transfer here was collected pursuant to a privacy policy which places few restrictions on how non-sensitive PII may be transferred pursuant to a bankruptcy proceeding. In many cases, the only relevant restriction was a promise to provide data subjects with a notice of any change in control over Debtor's PII assets – and that such notice would be provided via Debtors' Digital Properties or via email.

16. The CareerBuilder privacy policy advises visitors to the CareerBuilder Digital Properties of the possibility of a transfer of data pursuant to a bankruptcy or similar change in control. However, the privacy policy also promised that CareerBuilder customers "may opt-out of the sale of [] personal information." While the opt-out out of sale language could be construed to apply solely to the PII of data subjects located in California or another U.S. state with a comprehensive privacy law, it's unclear whether a reasonable consumer would interpret the language quite so narrowly the way it is drafted. At the very least, the Privacy Ombudsman believes that visitors to Debtors' CareerBuilder Digital Properties should receive a notice of

the change in control of their PII pursuant to this proceeding as well.

### **Sensitive Data**

17. However, when it comes to sensitive PII, the Debtor’s privacy policies promise that Debtor “will not use [s]ensitive [i]nformation for a purpose other than a purpose for which it was originally collected or subsequently authorized by the individual unless [Debtor] has received your affirmative and explicit consent (opt-in).” Debtors’ privacy policies provide some examples of what data Debtors consider to be sensitive, including “information about medical or health conditions, racial or ethnic origin, political opinions and religious or philosophical beliefs.” While those are clearly designed to serve only as examples, the Ombudsman notes that at least some of the data that Debtors collect would also be considered to be sensitive and/or subject to special processing considerations under applicable law in certain jurisdictions, such as age (to the extent the data subject is 16 or 17). Moreover, the Ombudsman believes that information about a person’s salary, job prospects, and prospective employment evaluations – while not “sensitive” under applicable law, are nonetheless deserving of special protections to the extent that such information were used out of context of a prospective employment relationship.

18. Fortunately, the question regarding which PII collected by Debtor is considered sensitive would only be raised in the event that Debtors seek to transfer this information to a Purchaser that does not meet the definition of a Qualified Buyer (defined below) – as such transfer may exceed the scope of Debtors’ privacy promises as they pertain to sensitive data.

19. Based on assurances provided by Debtors’ counsel, it is the Privacy Ombudsman’s understanding that the PII is likely (but not certain) to be transferred to a “Qualified Buyer.”

A “Qualified Buyer” means an entity that: (i) concentrates in the same business and market as Debtor; (ii) expressly agrees to be Debtors’ successor-in-interest as to the customer information; (iii) agrees to be responsible for any violation of that policy following the date of purchase; and (iv) shall not disclose, sell, or transfer customers’ PII to any third party in a manner inconsistent with Debtors’ Privacy Policy.

### **Recommendations**

20. Based on the foregoing, the Ombudsman respectfully submits the following recommendations to the Court:

21. First, the Court should approve the transfer of all PII from Debtors to Purchaser(s);

22. Second, in accordance with governing law permitting the transfer of PII, the Court should require that:

- a. Each Purchaser(s) shall represent to the Court that it is a Qualified Buyer with respect to the PII it receives pursuant to this proceeding;
- b. As the transfer of PII is to a “Qualified Buyer”: A “Qualified Buyer” means an entity that: (i) concentrates in the same business and market as Debtor; (ii) expressly agrees to be Debtors’ successor-in-interest as to the customer information; (iii) agrees to be responsible for any violation of that policy following the date of purchase; and (iv) shall not disclose, sell, or transfer customers’ PII to any third party in a manner inconsistent with Debtors’ Privacy Policy without obtaining each customer’s prior affirmative (“Opt-in”) consent;
- c. Debtors shall provide a notice of the change of control over Debtors’ PII via email and via its Digital Properties (e.g., via the privacy policies of such Digital Properties) and such privacy notice shall clearly explain that customer PII is being transferred

to Purchaser(s) and shall advise those consumers of the privacy rights that may be available to them under applicable U.S. state privacy laws;

- d. Debtors and Purchaser(s) shall cooperate with respect to maintaining records of data subject requests for a period of 24 months to ensure compliance with the requirements of the Colorado Privacy Act.<sup>10</sup>

23. Third, to the extent that one or more Purchaser(s) is unable to represent that it is a Qualified Buyer with respect to Debtors' PII, the Privacy Ombudsman will need to re-evaluate and issue a supplemental report with recommendations for stronger privacy protections depending on the Purchaser's line of business and the sensitivity of the PII subject to transfer, including but not limited to recommending: (i) a notice and opt-out choice privacy ruleset, or (ii) a notice and affirmative opt-in consent privacy ruleset.

24. Finally, the Order approving the sale of PII in this instance should also (i) require Purchaser(s) to each file with the Court a statement under oath that it has fully complied with the conditions imposed to protect the PII, including that Purchaser(s) are able to meet the definitional requirements of a Qualified Buyer; (ii) direct the Ombudsman to file a supplemental report confirming such compliance; or (iii) both.

### **Applicable Consumer Privacy and Data Protection Laws**

25. In the United States, the "privacy" of consumers' personally identifiable information has primarily been regulated by the Federal Trade Commission ("FTC") under the FTC Act, the Children's Online Privacy Protection Act of 1998 ("COPPA"), and the Gramm- Leach-Bliley Act ("GLBA"). There are a number of additional sectoral privacy laws which are not relevant

---

<sup>10</sup> See CPA Regulations Rule 6.11(B).

to this proceeding. Over the past few years, various U.S. states have created their own privacy laws which may be relevant.

### **U.S. Federal Laws**

26. The FTC Act - Section 5 of the FTC Act declares unfair or deceptive practices in commerce as unlawful.<sup>11</sup> To determine whether section 5's prohibition against deception has been violated, the FTC will first identify what "express claims," and "implied claims," have been made by a company.<sup>12</sup> An "express claim" refers to a factual assertion made in an advertisement or promotion or other publicly available statement such as a corporate policy. An "implied claim" refers to the net impression conveyed by all elements of a company's policies or statements "including an evaluation of such factors as the entire document, the juxtaposition of various phrases in the document, the nature of the claim, and the nature of the transactions." Section 5 is violated when an express or implied claim is "likely to affect a consumer's choice of or conduct regarding a product" and is "likely to mislead reasonable consumers under the circumstances."<sup>13</sup> In addition, an act or practice may be considered "unfair" if it causes, or is likely to cause, substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers.<sup>14</sup>

---

<sup>11</sup> 15 USC §45 (2006).

<sup>12</sup> FTC Policy Statement on Deception, *appended to Cliffdale Associates, Inc.*, 103 FTC 110, 174 (1984), available at <http://www.ftc.gov/bcp/policystmt/ad-decept.htm> (last visited July 10, 2025).

<sup>13</sup> *Id.*

<sup>14</sup> *See generally* FTC Policy Statement on Unfairness, *appended to International Harvester Co.*, 104 FTC 949, 1070 (1984) available at <http://www.ftc.gov/bcp/policystmt/ad-unfair.htm> (last visited July 10, 2025).

27. The FTC has explicitly applied section 5's prohibitions against deceptive acts and practices to corporate privacy statements made on the Internet and elsewhere in over a dozen consent orders.<sup>15</sup> The FTC has also cited companies for collecting consumers' information and then retroactively changing a privacy policy to allow such company to share the information with third parties without notifying consumers or getting their consent.<sup>16</sup>

28. The FTC order against *Toysmart* (discussed below and attached as **Exhibit N**) has particular significance here, as it brought about the amendment to the Bankruptcy Code that requires the appointment of the privacy ombudsman. As part of its settlement with Toysmart, the FTC noted the following: "[i]f the buyer wishes to make changes to that policy, it must follow certain procedures to protect consumers. It may not change how the information previously collected by Toysmart is used, unless it provides notice to consumers and obtains

---

<sup>15</sup> See, e.g., *United States v. ChoicePoint, Inc.*, Stipulated Final Judgment and Order (N.D. Ga. 2006) available at <http://www.ftc.gov/os/caselist/choicepoint/0523069stip.pdf> (last visited July 10, 2025); *In the Matter of Vision I Properties d/b/a CartManager International*, Agreement Containing Consent Order (FTC 2004) available at <http://www.ftc.gov/os/caselist/0423068/050310agree0423068.pdf> (last visited July 10, 2025); *In the Matter of Petco Animal Supplies, Inc.*, Decision and Order (FTC 2005) available at <http://www.ftc.gov/os/caselist/0323221/050308do0323221.pdf> (last viewed July 12, 2023); *In the Matter of Gateway Learning Corp.*, Decision and Order (FTC 2004) available at <http://www.ftc.gov/os/caselist/0423047/040917do0423047.pdf> (last visited July 10, 2025); *In the Matter of Tower Records*, Decision and Order (FTC 2004) available at <http://www.ftc.gov/os/caselist/0323209/040602do0323209.pdf> (last visited July 10, 2025); *In the Matter of Educational Research Center of America, Inc and Student Marketing Group, Inc.*, Decision and Order (FTC 2002) available at <http://www.ftc.gov/os/2003/01/ercaconsent.htm> (last viewed July 12, 2023); *In the Matter of the National Research Center for College and University Admissions, Inc.*, Decision and Order, (FTC 2003) available at <http://www.ftc.gov/os/2003/01/nrcuamuncedo.htm> (last visited July 10, 2025); *In the Matter of Microsoft Corporation*, Decision and Order (FTC 2002); *In the Matter of Eli Lilly and Company*, Decision and Order (FTC 2002) available at <http://www.ftc.gov/os/2002/05/elilillydo.htm> (last visited July 10, 2025); *FTC v. Reverseauction.com, Inc.*, Decision and Order (FTC 2000) available at <http://www.ftc.gov/os/2000/01/reverseconsent.htm> (last visited July 10, 2025); *In the Matter of Liberty Financial Co.*, Decision and Order (FTC 1999) available at <http://www.ftc.gov/os/2000/01/reverseconsent.htm> (last viewed July 18, 2009); *In the Matter of Geocities*, Decision and Order (FTC 1999) available at <http://www.ftc.gov/os/1999/02/9823015.do.htm> (last visited July 10, 2025).

<sup>16</sup> See, e.g., *Gateway Learning Corp.*, Decision and Order (FTC 2004) available at <http://www.ftc.gov/os/caselist/0423047/040917do0423047.pdf> (last visited July 10, 2025); and *In the Matter of IHEALTH.IO INC., a corporation, also d/b/a VITAGENE, INC.* Consent Order [https://www.ftc.gov/system/files/ftc\\_gov/pdf/decision\\_and\\_order.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/decision_and_order.pdf) (last viewed July 12, 2025).



their affirmative consent ("opt-in") to the new uses.”<sup>17</sup> In other words, the FTC position regarding a retroactive or material change to privacy practices is that such change would likely be actionable under Section 5 of the FTC Act unless opt-in consent were obtained.

29. The Privacy Policy Enforcement in Bankruptcy Act , also known as the Leahy-Hatch Amendment (“PPEBA”) is a federal law incorporated into the Bankruptcy Code through the Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (“BAPCPA”). Its purpose is to address concerns about the sale of personally identifiable information during bankruptcy proceedings, particularly when such sales contradict such company's existing privacy policies. The PPEBA effectively changed the Bankruptcy Code to create the position of Consumer Privacy Ombudsman and provide for the appointment of such Ombudsman where the debtor’s privacy policy places restrictions on the debtor’s ability to transfer such information.

30. The BAPCPA amendment to the Bankruptcy Code came as a result of the Federal Trade Commission’s (“FTC”) action against Toysmart.com, and incorporated aspects of the final (proposed) Stipulation and Order from that case. Some background on the Toysmart case might be helpful.

31. Toysmart Case. A casualty of the bursting of the Dot-Com bubble, Toysmart.com (“Toysmart”) had been engaged in the advertising, promotion, and sale of toys on the Internet.<sup>18</sup> In the course of doing business, Toysmart collected information from its customers, including, among other things, its customers’ names, addresses, billing information, and

---

<sup>17</sup> See the FTC press release announcing the Toysmart settlement at <https://www.ftc.gov/news-events/news/press-releases/2000/07/ftc-announces-settlement-bankrupt-website-toysmartcom-regarding-alleged-privacy-policy-violations> (last viewed July 12, 2025).

<sup>18</sup> See First Amended Complaint, Civil Action No. 00-11341 at ¶ 6 (D. Mass. 2000) *available at* <http://www.ftc.gov/os/2000/07/toysmartcomplaint.htm> (last viewed July 10, 2025).

shopping preferences. Toysmart’s website included a privacy policy which assured customers that Toysmart “never shared [its customers’ PII] with a third party.”<sup>19</sup>

32. When Toysmart sought to sell the PII of its customers as part of its Plan of Liquidation, in direct contravention of its privacy policy, the FTC charged Toysmart with engaging in a deceptive trade practice, in violation of Section 5 of the FTC Act,<sup>20</sup> and with violating COPPA,<sup>21</sup> because its customer data included the PII of children under the age of 13.

33. Although the FTC entered into a Stipulation and Settlement that would enable Toysmart to sell its customers’ PII under certain conditions, forty-six (46) States’ Attorneys General (and two of the FTC’s own commissioners) objected, arguing that “never” (as represented in Toysmart’s privacy policy) should mean “never” and that Toysmart should not be permitted to sell its customers’ PII under any circumstances.<sup>22</sup>

34. Ultimately, Toysmart withdrew the sale, and one of its equity owners, Disney, paid \$50,000 for the data and destroyed such data. The terms of the Stipulation and Settlement into which it had entered with the FTC established the criteria to determine the propriety of the transfer of customer PII assets in a bankruptcy proceeding, where the privacy policy does not address that situation and/or places restrictions on the debtor’s ability to sell its PII.

35. The Stipulation and Settlement provided that Toysmart’s customers’ PII would be sold only to a “Qualified Buyer,” an entity that (a) concentrates in the same business and market as Toysmart; (b) expressly agrees to be Toysmart’s successor-in-interest as to the customer

---

<sup>19</sup> *Id.* at ¶ 7.

<sup>20</sup> 15 U.S.C. §§45 *et seq.*

<sup>21</sup> Discussed below.

<sup>22</sup> The States’ objections rested primarily upon their own “mini-FTC Acts,” which prohibited deceptive acts or practices.

information; (c) agrees to be responsible for any violation of that policy following the date of purchase; (d) will use the PII only to fulfill customer orders and to personalize customers' experience on the website; and (e) shall not disclose, sell, or transfer customers' PII to any third party without giving the customers notice and an opportunity to opt-in to the transfer.<sup>23</sup> For the Court's convenience, a true and accurate copy of the FTC's proposed Stipulation and Settlement with Toysmart is attached hereto as **Exhibit N**.

36. The Qualified Buyer criteria have generally been followed in many subsequent bankruptcy cases.<sup>24</sup>

37. The Children's Online Privacy Protection Act ("COPPA"). In addition to the FTC Act, COPPA prohibits unfair or deceptive acts or practices in connection with the collection, use, or disclosure of personally identifiable information from and about children under age 13 obtained via the Internet.<sup>25</sup> COPPA requires that companies that collect information from children provide notice on their websites concerning what information they collect, how they will use that information, and what disclosure practices they apply to that information.<sup>26</sup> COPPA also requires that regulated companies obtain verifiable parental consent prior to the

---

<sup>23</sup> See Stipulation and [Proposed] Order Establishing Conditions on Sale of Customer Information, Civil Action No. 00-13995 (Bkr. D. Mass. 2000) available at <http://www.ftc.gov/os/2000/07/toysmartbankruptcy.1.htm> (last viewed July 11, 2018).

<sup>24</sup> In re Borders Group, Inc., No. 11-10614-mg (Bankr. S.D.N.Y.) (Glenn, J.), In re RadioShack Corporation, No. 15-10197 (BLS) (Bankr. D. Del.) (Shannon, J.); In re Choxi, 16-13131 (SCC) (Bankr. S.D.N.Y.) (Chapman, J.); In re Century 21 Department Stores, 20-12097 (Bankr. S.D.N.Y.) (Chapman, J.); In re KB US Holding 20-22962 (SHL) (Bankr. S.D.N.Y.) (Lane, J.); In re MKJC Hyundai, 20-42283, (Bankr. S.D.N.Y.) (Mazer-Marino, J.); In re Loot Crate, 19-11791-BLS (Bankr. D. DE) (Shannon, J.); In re NovaSom, 19-11734 (BLS) (Bankr. D. DE) (Shannon, J.); In re Hobbico, 18-10055 (KG) (Bankr. D. DE) (Gross J.); In re Circuit City Stores, 3:08-bk-35653 (Bankr. E.D. VA) (Huennekens, J.); In re Linens N Things, 08-10832 (CSS) (Bankr. D. DE) (Sontchi, J.)

<sup>25</sup> 15 U.S.C. § 6501, *et seq.* (2006); 16 C.F.R. § 312 (2006). See also Children's Online Privacy Protection Rule, Final Rule, 64 Fed. Reg. 59888 (Nov. 3, 1999) (explaining basis and purpose of the Act).

<sup>26</sup> 15 U.S.C. 6502(b)(1)(A) (2006); 16 C.F.R. § 312.3(a) (2006).

collection of information from children.<sup>27</sup> Pursuant to the FTC’s rules interpreting COPPA, a company must, among other things, obtain parental consent “to any material change in the collection, use, and/or disclosure practices to which the parent has previously consented.”<sup>28</sup> The FTC has interpreted COPPA as also applying to operators of websites that have actual knowledge that they are “maintaining” PII from children.<sup>29</sup>

38. In operating the Websites, the Debtors meet the definition of an “operator,” under both COPPA and the FTC’s rule promulgated pursuant thereto. An “operator” under COPPA is “any person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such website or online service ... where such website or online service is operated for commercial purposes, including any person offering products or services for sale through that website or online service, involving [interstate] commerce ....”<sup>30</sup>

39. Debtors’ Websites contain pages on which consumers are able to enter PII such as their name and email address to create and edit an account profile. Debtors collect date of birth, and Debtors’ privacy policies state that Debtors do not collect PII from persons under 16. Moreover, it is my understanding that Debtors have an age gate in place to ensure that persons under 16 could not provide PII to Debtors via the Websites. More importantly, the youngest age someone can generally work in the U.S. is 14 years old for non-agricultural jobs as per the Fair Labor Standards

---

<sup>27</sup> 15 U.S.C. 6502(b)(1)(A) (2006);

<sup>28</sup> 16 C.F.R. § 312.5(a) (2006).

<sup>29</sup> 16 C.F.R. § 312.3 (2009).

<sup>30</sup> 15 U.S.C. § 6501(2)(A)(i) and 16 C.F.R. § 312.2.

Act.<sup>31</sup> In other words, the Ombudsman was unable to identify a scenario whereby Debtors could have knowingly collected PII from a child under 13.

40. Given that it is extremely unlikely that the FTC would view Debtors' Websites as "child-directed" under COPPA, and that Debtors do not knowingly collect PII from persons under 16, COPPA is not implicated under the proposed sale.

41. The Gramm-Leach-Bliley Act ("GLBA") regulates the privacy of personally identifiable, nonpublic financial information disclosed to non-affiliated third parties by financial institutions. Among other things, the GLBA requires that regulated companies notify consumers of their privacy policies and provide them with notice and the opportunity to opt-out of changes to those policies. The Debtors have provided no information to indicate that they are a financial institution under the GLBA. Nevertheless, the FTC's rules, regulations, and interpretation of when the GLBA requires notification and opt-out may be informative in this situation.

42. During the FTC's consideration of its Privacy of Consumer Financial Information Rule, some entities that submitted comments requested guidance concerning "what notices are required in the event of a merger of two financial institutions or an acquisition of one financial institution by another."<sup>32</sup> In its comments on the final rule, the FTC indicated that in merger or acquisition scenarios:

---

<sup>31</sup> 29 U.S.C. § 203

<sup>32</sup> Privacy of Consumer Financial Information, Final Rule, 65 Fed. Reg. 33660 (May 24, 2000).

... [T]he need to provide new initial (and opt-out) notices to the customers of the entity that ceases to exist will depend on whether the notices previously given to those consumers accurately reflect the policies and practices of the surviving entity. If they do, the surviving entity will not be required under the rule to provide new notices.<sup>33</sup>

The FTC's interpretation of the GLBA as not requiring notice (and opt-out) in situations in which an acquirer adopts the policies and practices of the former company is consistent with the FTC's stipulation and decree in *Toysmart* as well as the Ombudsman's Recommendations to the Court.

### **Applicable U.S. State Laws**

43. State Consumer Protection Laws. Most states have consumer protection laws that are consistent with the FTC Act. Debtors' PII contains data on consumers in every U.S. state. If the proposed PII transfer satisfies the FTC transfer requirements, state consumer protection laws should likewise be satisfied.

44. State Privacy Laws. Several U.S. states have passed comprehensive privacy laws which are relevant to these proceedings, including but not limited to: California, Colorado, Connecticut, Delaware, Virginia and Utah.<sup>34</sup> These state privacy laws generally impose a notice and opt-out choice ruleset on the transfer or sale of non-sensitive personal information to third-parties. Moreover, a few of these state privacy laws contain provisions that contemplate the transfer of PII pursuant to a bankruptcy proceeding which may be relevant to this proceeding.

---

<sup>33</sup> *Id.* at 33660-33661.

<sup>34</sup> See <https://oag.ca.gov/privacy/ccpa> (California), <https://coag.gov/resources/colorado-privacy-act/> (Colorado), <https://portal.ct.gov/AG/Sections/Privacy/The-Connecticut-Data-Privacy-Act> (Connecticut), <https://legis.delaware.gov/BillDetail?LegislationId=140388> (Delaware), <https://www.oag.state.va.us/consumer-protection/files/tips-and-info/Virginia-Consumer-Data-Protection-Act-Summary-2-2-23.pdf> (Virginia), and <https://le.utah.gov/~2022/bills/static/SB0227.html> (Utah).

45. California Consumer Privacy Act. The California Consumer Privacy Act only considers the transfer of PII pursuant to a bankruptcy a “sale” of personal information in the event that the acquirer “materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection...” and in such case “it shall provide prior notice of the new or changed practice to the consumer.”<sup>35</sup>

46. Moreover, a recent enforcement action by California’s Office of the Attorney General (OAG) has taken the position that the CCPA’s “purpose limitation” principle could impose additional privacy requirements on a particular data set in the context of a sale of personal information.<sup>36</sup> The enforcement action, and the OAG’s analysis of the purpose limitation principle may be relevant. The purpose limitation principle limits a businesses’ use of personal information only for purposes for which it was collected, or for other purposes that are consistent with consumers’ reasonable expectations.<sup>37</sup> In that way, the CCPA has been interpreted by the OAG as to impose an opt-in consent standard where a potentially sensitive data set is used for a different purpose than under which it was collected – which is similar to a situation where data was transferred to an entity that does not meet the criteria of a Qualified Buyer.

---

<sup>35</sup> See CCPA Section 1798.140(ah)(2)(c) at [https://coppa.ca.gov/regulations/pdf/ccpa\\_statute.pdf](https://coppa.ca.gov/regulations/pdf/ccpa_statute.pdf) (last visited on July 10, 2025).

<sup>36</sup> See CCPA Section 1798.100(a)(1) at [https://coppa.ca.gov/regulations/pdf/ccpa\\_statute.pdf](https://coppa.ca.gov/regulations/pdf/ccpa_statute.pdf) (last visited on July 16, 2025). “A business shall not collect additional categories of personal information or use personal information collected for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected without providing the consumer with notice consistent with this section.”

<sup>37</sup> See CCPA Regulations § 7002 [https://coppa.ca.gov/regulations/pdf/20230329\\_final\\_regs\\_text.pdf](https://coppa.ca.gov/regulations/pdf/20230329_final_regs_text.pdf) (last visited on July 16, 2025) and *The People of the State of California v. Healthline Media, LLC* (CGC-25-626794) pages 7 & 8 <https://oag.ca.gov/system/files/attachments/press-docs/People%20v.%20Healthline%20Media%20Complaint.pdf> (last visited on July 16, 2025).

47. Colorado Privacy Act. The Colorado Privacy Act (CPA) does not consider the transfer of PII pursuant to a bankruptcy to be a “sale” of personal data.<sup>38</sup> However, the CPA imposes a rather unique rule under the CPA Regulations - which requires that the acquirer maintain copies of data subject access requests for a period of 24 months.<sup>39</sup> Accordingly, the Recommendations included in this Report include a reminder of the requirements set out in this provision of the CPA Regulations.

48. Virginia Consumer Data Protection Act. The Virginia Consumer Data Protection Act (VCDPA) also contemplates the transfer of data in the context of a bankruptcy proceeding. However, the VCDPA does not consider the transfer of PII pursuant to a bankruptcy as a “sale” of personal data as the term “sale” is defined under the VCDPA.<sup>40</sup>

49. Overall. Other than California’s and Virginia’s VCDPA rules, and Colorado’s CPA requirement to store data subject access requests for 24 months, the scope of U.S. state privacy laws does not specifically address the transfer of personal information pursuant to a bankruptcy proceeding. However, these state laws nonetheless impose certain requirements upon entities that collect and otherwise process the personal information of consumers. These requirements include: (a) honoring data subject access, deletion, and (in some cases) correction rights,<sup>41</sup> (b)

---

<sup>38</sup> See CPA Section 6-1-1303 at [https://coag.gov/app/uploads/2022/01/SB-21-190-CPA\\_Final.pdf](https://coag.gov/app/uploads/2022/01/SB-21-190-CPA_Final.pdf) (last visited on July 10, 2025). The transfer of PII pursuant to a bankruptcy is therefore not subject to the notice and choice requirements under the CPA.

<sup>39</sup> See CPA Regulations Rule 6.11(B) <https://coag.gov/app/uploads/2023/03/FINAL-CLEAN-2023.03.15-Official-CPA-Rules.pdf> (last visited on July 10, 2025). “Controllers shall maintain a record of all Data Rights requests made pursuant to C.R.S. § 6-1-1306 with which the Controller has previously complied. Such records shall be retained for at least twenty-four (24) months and shall be made available at the completion of a merger, acquisition, bankruptcy, or other transaction in which a Third Party assumes control of Personal Data to ensure any new Controller continues to recognize the Consumer’s previously exercised Data Rights.”

<sup>40</sup> See VCDPA § 59.1-575 at <https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/>.

<sup>41</sup> See § 59.1-575 at <https://www.oag.state.va.us/consumer-protection/files/tips-and-info/Virginia-Consumer-Data-Protection-Act-Summary-2-2-23.pdf> (last visited on July 10, 2025). For example, the Virginia Consumer Data Protection Act (VCDPA) allows for consumers to request that the controller of their personal data:



providing a privacy notice and opt-out choice regarding any sales of non-sensitive personal data,<sup>42</sup> (c) conducting privacy impact assessments,<sup>43</sup> and (d) the implementation of written data processing agreements.<sup>44</sup>

50. More importantly, certain state laws (as well as the FTC) view “material changes” in privacy practices as requiring the consumer’s affirmative opt-in consent. Fortunately, by ensuring that the sale of PII is to a Qualified Buyer, Debtors should eliminate the possibility of any FTC or state enforcement agency claiming that the sale of PII being transferred here constitutes a material change in privacy practices.

51. Data Controller vs Data Processor role. Finally, U.S. state privacy laws generally create role-based rules for entities seeking to process personal data whereby the applicable ruleset depends on an entities role in processing a particular data set. Given that Ombudsman’s recommendations to the Court are contingent upon Debtors’ processing role with respect to PII, the Report will explain privacy roles and how such roles impact the Ombudsman’s

- 
- Confirm if the controller is actually processing their personal data.
  - Correct inaccuracies in the consumer’s personal data that is collected by the controller.
  - Delete personal data provided by or obtained about the consumer.
  - Obtain copies of the personal data collected by the controller.
  - Opt out of the processing of personal data for purposes of targeted advertising, the sale of personal data, or further profiling.

<sup>42</sup> See <https://oag.ca.gov/privacy/ccpa#sectionb> (last visited on July 16, 2025). The California Consumer Privacy Act (CCPA, as amended) requires that businesses provide a privacy notice and right to opt-out from the sale or sharing of personal information.

<sup>43</sup> See [https://coag.gov/app/uploads/2023/01/CPA\\_Version-3-Proposed-Draft-Regulations-1.27.2023.pdf](https://coag.gov/app/uploads/2023/01/CPA_Version-3-Proposed-Draft-Regulations-1.27.2023.pdf) (last visited on July 10, 2025). The draft rules for the Colorado Privacy Act promulgated by the Colorado Attorney General’s office states that: “A data protection assessment shall be a genuine, thoughtful analysis of each Processing activity that presents a heightened risk of harm to a Consumer, that: 1) identifies and describes the risks to the rights of consumers associated with the processing; 2) documents measures considered and taken to address and offset those risks, including those duties required by C.R.S. § 6-1-1308; 3) contemplates the benefits of the Processing; and 4) demonstrates that the benefits of the Processing outweigh the risks offset by safeguards in place.

<sup>44</sup> See [https://cppa.ca.gov/regulations/pdf/20221102\\_mod\\_text.pdf](https://cppa.ca.gov/regulations/pdf/20221102_mod_text.pdf) (last visited on July 10, 2025). The California Consumer Privacy Act (CCPA, as amended) requires a written contract when personal data is shared in most circumstances.

evaluation.

52. A controller of personal data (sometimes referred to as data controller or a business<sup>45</sup>) determines the purposes and means of processing personal data. For the most part, Debtors operate as a controller of PII in that it is Debtors that make the decisions for how PII they've collected is processed.

53. A processor of personal data (sometimes referred to as a data processor or a “service provider”<sup>46</sup>) receives its processing instructions from the controller of the data set and may only process such data as directed by the controller. In some instances (e.g., where Debtors offer to customers a white-label version of its services), Debtors operate as a data processor. Where Debtors are a data processor, the Debtors are both contractually and legally bound to process the PII as directed by Debtors' customers (each, a data controller of such PII).

54. Where Debtors are transferring PII for which Debtors are a data processor pursuant to this bankruptcy proceeding, the processing decisions are not impacted as the Purchaser will be also be bound as a data processor and will be legally required to process such PII as instructed by each respective customer. Accordingly, the transfer of such PII here is not subject to review by the Privacy Ombudsman.

### **Non-U.S. Laws**

55. Debtors' counsel represented that while the Debtors did collect the personally identifiable information of customers from non-U.S. data subjects, none of this data is subject to transfer

---

<sup>45</sup> See the CCPA Section 1798.140(d) at [https://coppa.ca.gov/regulations/pdf/ccpa\\_statute.pdf](https://coppa.ca.gov/regulations/pdf/ccpa_statute.pdf) (last visited on July 16, 2025).

<sup>46</sup> See CCPA Section 1798.140(ag1) at [https://coppa.ca.gov/regulations/pdf/ccpa\\_statute.pdf](https://coppa.ca.gov/regulations/pdf/ccpa_statute.pdf) (last visited on July 10, 2025).

under the proposed sale. Accordingly, the “applicable nonbankruptcy law”<sup>47</sup> does not include the data protection laws of non-U.S. countries. If Debtors seek to transfer PII of non-U.S. data subjects to Purchaser(s) or another third-party as part of this proceeding, the Court should instruct the Ombudsman to file a supplemental Report.

### **The Debtors’ Consumer Privacy Policies and Practices**

56. A representative sample of Debtors’ privacy statements are attached to this Report as **Exhibits A through M**. Debtors have published several different privacy policies and have made edits to those privacy policies over time. Overall, Debtors’ privacy policies have consistently contemplated the transfer of customer information in the context of a bankruptcy, merger or similar business transaction. And for the most part, those policies promised that its customers would be provided with a notice of change in ownership or control of their PII.

57. However, when it comes to sensitive PII, the Debtor’s privacy policies promise that Debtor “will not use [s]ensitive [i]nformation for a purpose other than a purpose for which it was originally collected or subsequently authorized by the individual unless [Debtor] has received your affirmative and explicit consent (opt-in).” Debtors’ privacy policies provide some examples of what data Debtors consider to be sensitive, including “information about medical or health conditions, racial or ethnic origin, political opinions and religious or philosophical beliefs.” While those are clearly designed to serve only as examples, the Ombudsman notes that at least some of the data that Debtors collect would also be considered to be sensitive and/or subject to special processing considerations under applicable law in certain

---

<sup>47</sup> 11 USC §363(b)(1)(B)(ii) (2006)

jurisdictions, such as age (to the extent the data subject is 16 or 17). Moreover, the Ombudsman believes that information about a person's salary, job prospects, and prospective employment evaluations – while not “sensitive” under applicable law, are nonetheless deserving of special protections to the extent that such information were used out of context of a prospective employment relationship.

58. Fortunately, the issue of which PII collected by Debtor is considered sensitive would only come into question in the event that Debtors seek to transfer this information to one or more Purchaser(s) that does not meet the definition of a Qualified Buyer (defined below) – as such transfer may exceed the scope of Debtors' privacy promises as they pertain to sensitive data.

### **Factors to Be Considered**

59. Bankruptcy Code Section 332 suggests at least four factors as to which the Ombudsman may inform the Court: (a) Debtors' privacy policy; (b) potential losses or gains of privacy to consumers if a sale is approved; (c) the potential costs or benefits to consumers if such sale is approved; and (d) potential alternatives that would mitigate potential privacy losses or potential costs to consumers.<sup>48</sup>

60. Debtors' Privacy Policies - As discussed above, Debtors' privacy policies generally address the transfer of data in a bankruptcy proceeding – and promise to provide a notice of change in ownership or control. Provided that Purchaser is a Qualified Buyer with respect to Debtors' PII, the Debtor would not be viewed as violating its privacy policy promises.

---

<sup>48</sup> 11 U.S.C. §332.

61. Potential Losses, Gains and/or Costs to Privacy if the Sale is Approved - Similarly, the transfer of consumer PII contemplated here will have a minimal impact upon consumers provided that the Purchaser is a Qualified Buyer. The transfer of PII to Purchaser would only result in a loss of privacy to the consumers involved if Purchaser were to adopt significantly different privacy practices from that employed by Debtors.

62. Mitigating Potential Privacy Losses - The best way in which to mitigate potential privacy losses to Debtors' customers is to require Purchaser to continue to meet consumers' privacy expectations. The general outline of those requirements has been provided in FTC enforcement actions, guidance and cases such as *Toysmart*. The proposed requirements with respect to Debtors' proposed transfer are set forth below.

### **Recommendations**

63. Based on the foregoing, the Ombudsman respectfully submits the following recommendations to the Court:

64. First, the Court should approve the transfer of all PII from Debtors to Purchaser(s);

65. Second, in accordance with governing law permitting the transfer of PII, the Court should require that:

- a. Each Purchaser(s) shall represent to the Court that it is a Qualified Buyer with respect to the PII it receives pursuant to this proceeding;
- b. As the transfer of PII is to a "Qualified Buyer": A "Qualified Buyer" means an entity that: (i) concentrates in the same business and market as Debtor; (ii) expressly agrees to be Debtors' successor-in-interest as to the customer information; (iii) agrees to be responsible for any violation of that policy following the date of purchase; and (iv)

shall not disclose, sell, or transfer customers' PII to any third party in a manner inconsistent with Debtors' Privacy Policy without obtaining each customer's prior affirmative ("Opt-in") consent;

- c. Debtors shall provide a notice of the change of control over Debtors' PII via email and via its Digital Properties (e.g., via the privacy policies of such Digital Properties) and such privacy notice shall clearly explain that customer PII is being transferred to Purchaser(s) and shall advise those consumers of the privacy rights that may be available to them under applicable U.S. state privacy laws;
- d. Debtors and Purchaser(s) shall cooperate with respect to maintaining records of data subject requests for a period of 24 months to ensure compliance with the requirements of the Colorado Privacy Act.<sup>49</sup>

66. Third, to the extent that one or more Purchaser(s) is unable to represent that it is a Qualified Buyer with respect to Debtors' PII, the Privacy Ombudsman will need to re-evaluate and issue a supplemental report with recommendations for stronger privacy protections depending on the Purchaser's line of business and the sensitivity of the PII subject to transfer, including but not limited to recommending: (i) a notice and opt-out choice privacy ruleset, or (ii) a notice and affirmative opt-in consent privacy ruleset.

---

<sup>49</sup> See CPA Regulations Rule 6.11(B).

67. Finally, the Order approving the sale of PII in this instance should also (i) require Purchaser(s) to each file with the Court a statement under oath that it has fully complied with the conditions imposed to protect the PII, including that Purchaser(s) are able to meet the definitional requirements of a Qualified Buyer; (ii) direct the Ombudsman to file a supplemental report confirming such compliance; or (iii) both.

Dated: July 16, 2025

/s/Alan Chapell  
ALAN CHAPELL